References

[1] A. Tamersoy, K. Roundy and D. H. Chau (2014) “Guilt by association: large scale malware detection by mining file-relation graphs”, “ACM 20th International Conference on Knowledge Discovery and Data Mining”, pp. 1524-1533

[2] Anderson HS, Roth P. EMBER (2018) “An Open Dataset for Training Static PE Malware Machine Learning Models”. arXiv preprint arXiv:1804.04637

[3] B. Anderson, D. Quist, J. Neil, C. Storlie and T. Lane (2011) “Graph-based malware detection using dynamic analysis”, “Journal in Computer Virology”, Vol. 7, Issue 4, pp.247-258.

[4] Buczak AL, Guven E.(2016) “A survey of data mining and machine learning methods for cyber security intrusion detection”. “IEEE Communications Surveys & Tutorials”. 18, (2):1153-76.

[5] E. Gandotra, D. Bansal, S. Sofat,(2014) “Malware analysis and classification: A survey”, “Journal of Information Security”, Vol.5, Issue 2 , pp. 56-64.

[6] Emm, D., Garnaeva, M., Unuchek, R., Makrushin, D., & Ivanov, A. (2014). “IT THREAT EVOLUTION IN Q3” 2015.

[7] F. Shahzad, M. Shahzad and M. Farooq,(2013) “In-execution Dynamic Malware Analysis and Detection by Mining Information in Process Control Blocks of Linux Operating System”, “Data Mining for Information Security”, Vol. 231, pp.45-63

[8] Fausett, L.(1994) “Fundamentals of neural networks: architectures, algorithms, and applications”.

[9] Felt, A. P., Finifter, M., Chin, E., Hanna, S., & Wagner, D. (2011). “A survey of mobile malware in the wild. In Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices” (pp. 3-14). ACM.

[10] G. S.Tangil, J. E. Tapiador, P. P.Lopez, and A. Ribagorda,(2014) “Evolution, Detection and Analysis of Malware for Smart Devices”, “IEEE Journal of Communications Surveys & Tutorials”, Vol. 16, Issue 2, pp.961-987.

[11] H. Gascon, F. Yamaguchi, D. Arp. and K. Rieck,(2013) “Structural Detection of android Malware using Embedded call graphs”, “Conference on Artificial intelligence and security”, pp. 45-54.

[12] A. Saeed, A. Semant, A. M.A. Abuagoub,(2013) “A Survey on Malware and Malware Detection Systems”, “International Journal of Computer Applications”, Vol. 67, Issue 16, pp. 25-31.

[13] Santos, J. Devesa, F. Brezo, J. Nieves, and P. G Bringas,(2013) “Opem: A static-Dynamic approach for machine-learning-based Malware Detection”, “International Joint Conference CISIS” 12-ICEUTE´ 12-SOCO´ 12 Special Sessions, Vol. 189,pp. 271-280.

[14] J. Landage, Prof. M. P. Wankhade, “Malware and Malware Detection Techniques: A Survey”,(2013) “International Journal of Engineering Research & Technology (IJERT)”, Vol. 2 , Issue 12, pp. 1-8.

[15] J. Rabek, R. Khazan, S. Lewandowski and R. Cunningham,(2013) “Detection of injected, dynamically generated, and obfuscated malicious code”, “Proceedings of the ACM Workshop on Rapid Malcode”, USA, pp. 76–82.

[16] K. Allix, Q. Jerome, T.F. Bissyande, J. Klein, R. State and Y.L. Traon,(2014) “A Forensic Analysis of Android Malware--How is Malware Written and How it Could Be Detected?”, 38th “IEEE Annual Computer Software and Applications Conference” (COMPSAC), Vasteras, pp. 384-393.

[17] K. Harrison , B. Bordbar , S. T. T. Ali , C. I. Dalton , A. Norman,(2012) “A framework for detecting malware in cloud by identifying symptoms”, “16th IEEE International Enterprise Distributed Object Computing Conference “ (EDOC), Beijing, pp.164-172.

[18] K. Mathur, S. Hiranwal, “A Survey on Techniques in Detection and Analyzing Malware Executables”,(2013) “International Journal of Advanced Research in Computer Science and software engineering”, Vol. 3, Issue 4.

[19] Kang, H., Jang, J. W., Mohaisen, A., & Kim, H. K. (2015). “Detecting and classifying android malware using static analysis along with creator information. International Journal of Distributed Sensor Networks”.

[20] M. Christodorescu, S. Jha, S. A Seshia, E Bryant,(2005) “Semantics-aware malware detection”, “IEEE Symposium on Security and Privacy”, pp. 32-46.

[21] M. Damshenas, A. Dehghantanha, R. Mahmoud,(2013) “A Survey on Malware Propagation, Analysis, and Detection”, “International Journal of Cyber-Security and Digital Forensics” (IJCSDF), Vol. 2 , Issue 4, pp.10-29.

[22] M. K. Shankarapani, S. Ramamoorthy, R. S. Movva and S. Mukkamala,(2011) “Malware Detection using Assembly and API call sequences”, “Journal in Computer Virology”, Vol.7, Issue 2, pp.107-119.

[23] M. Overton, “Anti-Malware Tools: Intrusion Detection Systems”,(2005) “EICAR conference”, Malta, pp. 1-22.

[24] M. Zubair Rafique and Juan Caballero,(2013) “Firma: Malware clustering and network signature generation with mixed network behaviors”, “In Research in Attacks, Intrusions, and Defenses”, Vol. 8145, pp. 144-163.

[25] M.S Alam and S.T. Vuong,(2013) “Random forest classification for Detecting Android Malware”, “IEEE conference on Green Computing and Communications (Green Com) and Internet of Things (I Things/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing”, Beijing, pp. 663-669.

[26] Mahindru A, Singh P.(2017) “Dynamic permissions based Android malware detection using machine learning techniques”. “In Proceedings of the 10th Innovations in Software Engineering Conference” Feb 5 (pp. 202-210). ACM

[27] Mahmassani, H., Williams, J. C., & Herman, R..(1984) “Investigation of network-level traffic flow relationships: some simulation results”.

[28] Milosevic N, Dehghantanha A, Choo KK.(2017) “Machine learning aided android malware classification”. “Computers & Electrical Engineering”. 1;61:266-74.

[29] N. Idika and A.P Mathur,(2007) “A Survey of Malware Detection Techniques,” “Department of Computer Science”, Purdue University, West Lafayette, pp. 1-48.

[30] Nix, R..(2017) “Applying Deep Learning Techniques to the Analysis of Android APKs”, Olin College of Engineering.

[31] P.V. Shijo, A. Salim,(2015) “Integrated Static and Dynamic Analysis for Malware Detection”, “International Conference on Information and Communication Technologies”, Kochi India, pp.804-811.

[32] Prasse, P., Gruben, G., Machlika, L., Pevny, T., Sofka, M., & Scheffer, T.. (2017) “Malware Detection by HTTPS Traffic Analysis”

[33] Rutkowska, J..(2006) “Introducing stealth malware taxonomy”. “COSEINC Advanced Malware Labs”, 1-9.

[34] S. Alam, R. N. Horspool and I. Traore,(2014) “MARD: A framework for metamorphic malware analysis and real-time detection”, 28th “IEEE International Conference on Advanced Information Networking and Applications (AINA)”, Victoria, pp. 480-489.

[35] S. Das, Y. Liu, W. Zhang, and M. Chandramohan(2016) ,“Semantics-Based Online Malware Detection: Towards Efficient Real-Time Protection Against Malware”, “IEEE transactions on information forensics and security”, Vol. 11, Issue 2, pp. 289 - 302.

[36] Shalaginov A, Banin S, Dehghantanha A, Franke K.(2018) “Machine learning aided static malware analysis: A survey and tutorial”. “Cyber Threat Intelligence”. pp. 7-45.

[37] U. Baldangombo, N. Jambaljav, and S. J. Horng,(2013) “A static Malware Detection system using Data Mining Methods”, arXiv preprint arXiv:1308.2831.

[38] V. M. Afonso, D. S. F. Filho, A. R. A. Gregio, P. L. de Geus, M. Jino,(2012) “A hybrid framework to analyze web and operating system malware”, “IEEE International Conference on Communications (ICC)”, Ottawa, pp. 966-970.

[39] Yang, X. S(2010)..” Nature-inspired metaheuristic algorithms”. Luniver press.,

[40] Z. Bazrafshan, H. Hashemi, S. M. H. Fard and A. Hamzeh,(2013) “A survey on heuristic malware detection techniques”, “5th IEEE Conference on Information and Knowledge Technology (IKT)”, pp. 113-120.

[41] Z. Chen, M. Roussopoulos, Z. Liang, Y. Zhang , Z. Chen and A. Deli, (2012)“Malware characteristics and Threats on the Internet Ecosystem”, “Journal of Systems and Software”, Vol. 85, Issue 7 , pp.1650-1672.